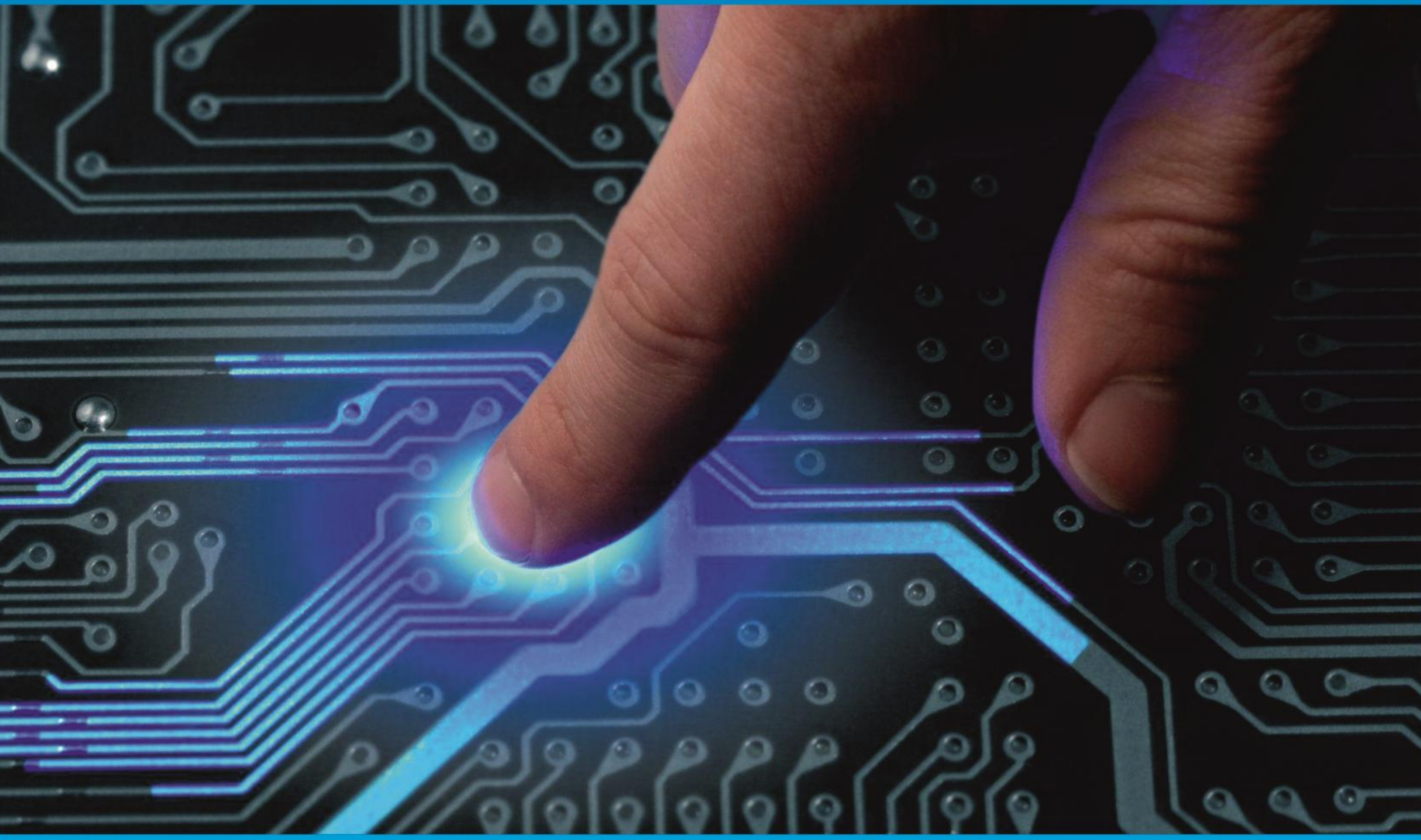
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165

| DOI: 10.15680/IJIRCCE.2022.1006159 |

Chaotic Digital Image Encryption Using Matlab

[1]A.Veerababu, [2*]Y.Varun Mahindra, [3]Y.Swvarajh Reddy, [4]V.Ravi Chandra

[1.]Assistant Professor, Department of Electronics and Communication Engineering St. Peter's Engineering College, Hyderabad, Telangana, India

[2,3,4]UG Student, Department of Electronics and Communication Engineering St. Peter's Engineering College, Hyderabad, Telangana, India

ABSTRACT: Security of the data which is being transferred at a daily basis is one of the major concerns of an individual today. Although there are predefined image encrypting algorithms they might not result in strong encryption as they will be easy to hack. Implementation of chaotic algorithms randomly generates a mathematical sequence using which image encryption can be more robust. Chaos maps and chaotic systems have been proved to be useful and effective for cryptography. The logistic map techniques used for image encryption tend to be more complicated in terms of codes and implementation. The proposed method adopts non linear 3D based chaos technique which makes use of position permutation and value transformation technique. The proposed method is able to provide an optimum entropy value as well. The co-relation coefficient value of horizontal and vertical position of cipher is compared with the standard encryption methods and also with the original image as well. The types of attacks, sensitivity and key space will also be discussed in the proposed approach.

KEYWORDS: Chaos map, secure cipher, Arnold Transform.

I. INTRODUCTION

In the era of rapid exchange of the information using various devices, data privacy and security has been a majorconcern to respect each individual safety and privacy.
Also, most of the data is transferred in a digital format although the initial data is analog to ensure the fast and robust data transfer. Mostly the data when transferred in case of government and military departments is supposed to be more safer than the general or random data transfer.

Therefore, the security protection of digital images has received great attention from all parties. Especially in the background of the increasingly severe network security situation in recent years, information transmission and sharing based on digital images often face the problems of data theft, tampering, deletion, and attack, which have caused great losses to the owners or publishers of digital images.
The perfect solution to ensure the safest and fastest data transfer in digital data transmission is to use a chaos sequence which uses a pseudo random sequence generator to give away the cipher text. The best way to ensure this is to use a 2D map.

The given algorithm makes use of overlapping blocks and shuffling images to generate the primitive cipher text of the given input. The next stage focuses on a chaotic map so as to generate a chaos and alter the same to the initial cipher.The Blow Fish algorithm is used so as to ensure an add on security as we support a colour image encryption in chaos. The dynamic S-Box is made use with a modifies F-function is used to generate a chaos map. Extending to the existing pseudo random sequence generators these operations increase the randomness and performance of cipher text.
The Arnold transform used shares a major contribution to the cipher text generation which uses the overlapping bocks and the sequences which are generated initially and hence iterates over the generated position permutational value and generates the cipher key iterated the n no of times where n is the user defined choice.

The Arnold Transform we have discussed shows optimum output when the provided image is a square image provided of equal boundaries. Hence it is essential to check whether the image is a square image or it is supposed to be converted into a square image. Let the height and width of an image be W,H we convert W=H by taking care of loss of generality. Through the method the plain-image is converted into a new image whose size is N×N. Due to the colour image that is composed of three colour components, we convert three components into three matrices, namely R, G, B.
The main objective behind the application of Arnold Transform is to increase the iterations to the m+L times where L is the size of the image and the value of m is set to 13 for our convenience.

Now this transform would generate more secure and iterated key using the chaos so that the output of the cipher would be of an improved randomness and also the higher efficiency while decrypting the image. Although the height of the image is unknown at the time of decryption Arnold transform helps in finding out the actual dimensions of the given image as we can yield the same while applying the inverse Arnold transform.

Two-dimensional Logistic Map

A discussed the 2D map used in generation of map using the chaotic pseudo random generation is as follows:
Each of the coordinates x, y is allocated a permutational values based on μ, ν values, which are the initial conditions which we have generated.

The map values are calculated using the formula as given below

$$\phi 1(x_n) = \mu_1 x_n(1 - x_n) + \nu_1 y_{2\,n}$$

$\phi 1(y_n) = \mu 2 y_n(1 - y_n) + \nu 2(x_{2\,n} + x_n y_n)(1)$

when $2.75 < \mu 1 \leq 3.4$, $2.75 < \mu 2 \leq 3.45$, $0.15 < \nu 1 \leq 0.21$ and $0.13 < \nu 2 \leq 0.15$, the system can generate pseudo numbers in the region (0,1]. All parameters are generated by key generator.

The Arnold Transform on an Image:

As we are ready with the mapped output of a cipher key and the position of each pixel in, we would further proceed with the Arnold Transform to ensure the security of the generated cipher text.

The formulated representation of given Arnold Transform is as shown

$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} A(mod(N))$..(2) where we set N=256. When a = b = 1, A=$\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$

. The secret key concept is involved here so as to improve the security of the given data. So the parameters a, b are used as secure keys in the Arnold Transformation.

The same process is considered in the decryption phase by converting the transform to inverse.

$$\begin{bmatrix} x \\ y \end{bmatrix} = A^{-n} \begin{bmatrix} x' - k\mu \\ y' - kv \end{bmatrix} (modN)$$

The process of arnold transform makes the image ready to be decrypted as it is not possible to decrypt the image without knowing the height and width of a original image.

Quantum Map using chaos:

The given chaos uses a modified quantum theory where the given pixels are given the cipher value based on the values of x and y we are considering and the "n" reperesents the position of the (x, y) coordinate in the given system.

The mathematical and formulated view of the given map using quantum theory is

$\phi 2(x'_n) = r(x'_n - |x'_n|^2) - ry'_n$ …(3)

$\phi 2(y'_n) = -y'_n \exp(-2\beta) + \exp(-\beta) r[(2 - x'_n - x'^*_n)y'_n - x'_n z'^*_n - x'^*_n z'_n]$ …(4)

$\phi 2(z'_n) = -z'_n \exp(-2\beta) + \exp(-\beta) r[2(1 - x'^*_n)z'_n - 2x'_n y'_n - x'_n]$ ….(5)

Coupling the Map using Nearest Neighbours

Now the chaos is generated using the quantum theory we need to map it to the corresponding pixel and the coordinate inthe given system. It is achieved by using the equations as given below. The x,y components are used to get Z components.

$z_{n+1}(j) = (1 - \varepsilon)\phi(z_n(j + 1)) + \varepsilon\phi(z_n(j + 1))$ ..(6)

$x_{n+1} = (1 - \varepsilon)\phi(x_n) + \varepsilon\phi(y_n)$ …..(7)

$y_{n+1} = (1 - \varepsilon)\phi(y_n) + \varepsilon\phi(x_n)$ ……(8)

Histogram of Encrypted Image

In the ideal characteristics of image encryption the histogram of an image is supposed to be uniform in terms of frequency distribution of the same. Hence when we consider the encrypted image cipher generated is independent on the grey scale and binary level of the image when considered to the input image. So this makes the algorithm more robust to any statistical attacks as significant yielding of data from cipher is more tedious. Correlation of Two Adjacent Pixels

The correlation of the adjacent pixels is necessarily done so that the pixels are tested and are made more secured in the cipher text so that the given cipher is cleanly generated and is not open to any statistical or brute force attacks which are done on the input plain image.

II LITERATURE SURVEY

Shaojun Zhong on A digital image encryption algorithm based on chaotic mapping[1] has proposed a chaotic map system based upon XZQ algorithm and also provides medium entropy. According to Shannon, the basic techniques for an encryption system can be classified into two main categories: diffusion and confusion. And the combination between the two classes is also possible. In the past few years, due to the close relationship between cryptography and chaos, some studies based on chaotic systems have been realized. The scheme based on chaotic system has the characteristics of pseudo-randomness, ergodicity and sensitivity to initial conditions, which ensures the security and efficiency of the system.
Limitations areNo iterations Over keys, which makes it low secured affecting the output**,** was published onJuly 1,2019

Hamedghazanfaripour on Designing a digital image encryption scheme using chaotic maps with prime modular [2] proposed an algorithm.This study proposes a scale-invariant digital image encryption method that includes three main steps rows-columns diffusion, the 3D scale-invariant modular chaotic map, and Hill diffusion. Pixels substitution, and mixing adjacency pixels of the plain image are performed using rows-columns diffusion and Hill diffusion. The 3D scale-invariant chaotic maps are used to permutation image pixels without image size restriction. Modular arithmetic is used in the 3D scale-invariant chaotic maps and Hill diffusion to increase keyspace and enhance security parameters.

Limitations areThe given system implements scale-invariant Modular Chaotic map Prime modular Diffusion Permutation**,** was published in the phrase of May,2020
Hailapan, Yon mei and Chiang jain in Research on digital image encryption algorithm based on double logistic chaotic map[3] have stated that the development of information technology, image information has become the main content of network information transmission. With the development of image encryption technology, it is also about the development of image information theft technology. In order to cope with the evolving information theft technology, we must seek a better image encryption algorithm. Among many algorithms, due to the superiority of chaos technology, when the image is encrypted with chaos technology, the ciphertext presents a randomness, which makes the possibility of deciphering greatly reduced.
Limitations are that The simulation experiments are carried out by using the results are analyzed from the histogram, pixel correlation, information entropy, key space size, key sensitivity, and so on, published on June 2018.
Kang Guoon A new image alternate encryption algorithm based on chaotic map [4] stated that A new image alternative encryption algorithm is proposed, in which the shuffling and diffusion are performed simultaneously. The plain image is divided into two left and right blocks of same size. The matrix which is generated by a logistic map is used to diffuse the left block of the plain image. Then, the diffused image is used as the right block of the cipher image. The 0, 1 sequence which comes from another logistic chaotic sequence and plaintext is used to shuffle the right block of the cipher image. After the operation XOR, the left block of cipher image is generated.
Limitations areLess sensitive to attacks ,published in February 2014.

III.PROPOSED SYSTEM

The proposed technique uses a mathematical iterative and bijection transform called Arnold Transform, we are supposed to convert the given image to a square image if it is found to be a rectangular one.
The image is firstly tested for the maximum value in the height or width in terms of dimension and the image is converted into a square format.
The given format of the Arnold transform increases the key sensitivity also the randomness of the given cipher text.
The given image is now yielded into the format of R,G,B phases so as to ensure a proper segmentation of the given pixels in the image as we are proceeding with the colour image encryption.
Permutation process:
The permutation process is the first phase of the given cryptosystem where the image pre processing and the R,G,B components are yielded.

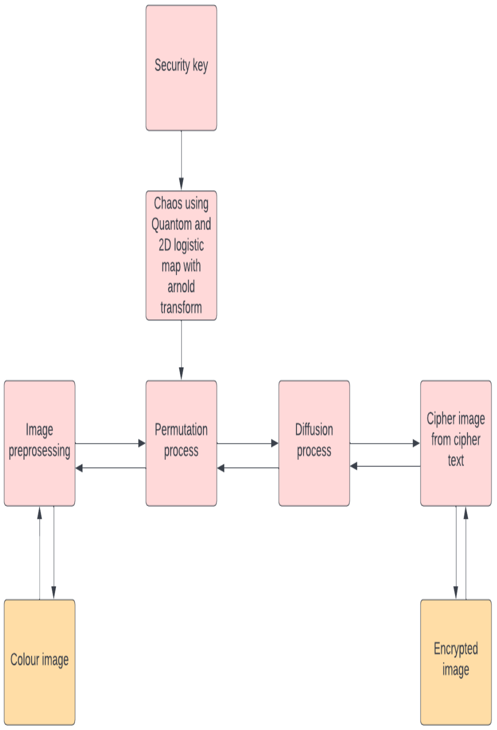
In the next consequent stage the 2D logistic map is used as chaos to generate the cipher text and the correlation, nearest neighbour coupling is used to increase the correlation, key space and the randomness of the generated chaos.

Now that we are done with the generation of chaos we have to generate the cipher image from the cipher text generated which is done using the diffusion process.

Diffusion process:

The diffusion process basically converts the cipher text to image by positioning the given texts at the suitable position by using the similar mapping algorithms we have used earlier taking care of the correlation of the pixels.

IV.BLOCK DIAGRAM

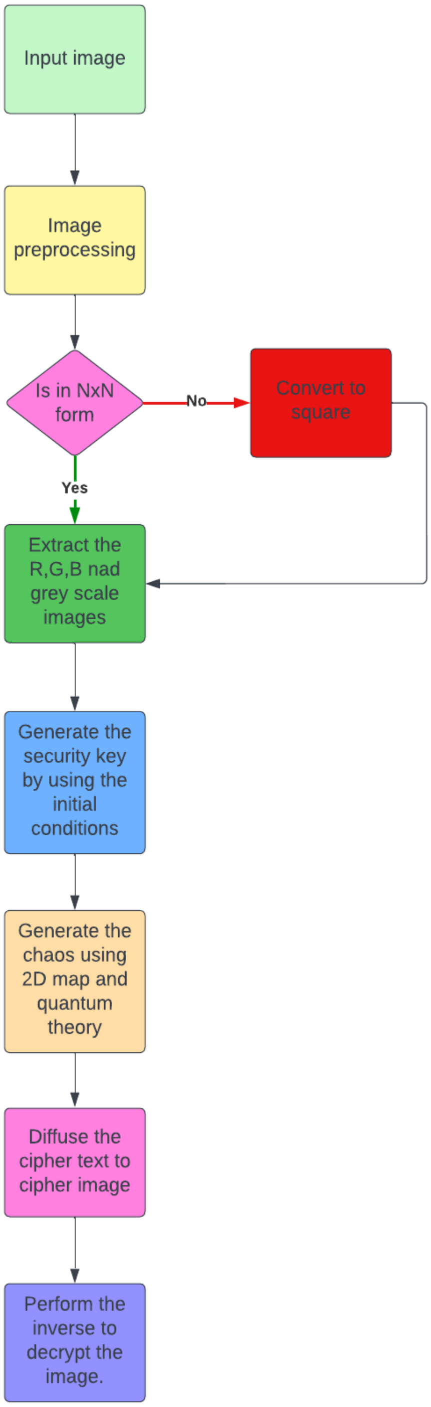


As shown in the above bock diagram the given image undergoes the pre processing, permutation, diffusion and cipher text generation. The same image can be reverted in case of decryption process as the arrows rightly indicate.

The encrypted image will be applied the inverse of the transformation we have seen in the cipher text generation process while we decode the same.

Hence the two way arrows are indicated to represent the inverse relation with the encryption and decryption phenomenon.

V.FLOW CHART


Input image
Image preprocessing
Is in NxN form
No
Convert to square
Yes
Extract the R,G,B nad grey scale images
Generate the security key by using the initial conditions
Generate the chaos using 2D map and quantum theory
Diffuse the cipher text to cipher image
Perform the inverse to decrypt the image.

VI.RESULTS

Fig.1 Input Image

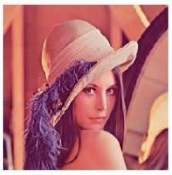


Fig 2 Decrypted Image

VII.CONCLUSION

In the proposed system the image encryption is highly robust and is also sensitive to the 2^128 planned or unplanned attacks. The proposed cryptosystem makes use of standard encryption and pseudo random sequence generating algorithms which generate chaos and is open to be encrypted “n” times as per the requirement of the user due to the utilisation of Arnold Transform.

The proposed cryptosystem generates a cipher text based on nearest neighbour coupling and the permutation, diffusion process also decrypts the same applying the inverse of the operated sequences by substituting the generated key in the initial steps.

REFERENCES

[1] A. Akhshani, A. Akhavan, S. C. Lim, and Z. Hassan, “An image encryption scheme based on quantum logistic map,” Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 12, pp. 4653– 4661, 2012.

[2] A. Akhshani, A. Akhavan, A. Mobaraki, S. C. Lim, and Z. Hassan, “Pseudo random number generator based on quantum chaotic map,” Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 1, pp. 101–111, 2014.

[3] F. Chen, K. W. Wong, X. Liao, and T. Xiang, “Period distribution of generalized discrete arnold cat map,” Theoretical Computer Science, vol. 552, no. 4, pp. 13–25, 2014.

[4] L. Chen, D. Zhao, and F. Ge, “Mage encryption based on singular value decomposition and arnold transform in fractional domain,” Optics Communications, vol. 219, no. 6, pp. 98–103, 2013.

[5] M. Ding and W. Yang, “Stability of synchronous chaos and on-off intermittency in coupled map lattices,” Physical Review E, vol. 56, no. 4, pp. 4009– 4016, 1997.

[6] A. A. A. El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, “A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces,” Signal Processing, vol. 93, no. 11, pp. 2986– 3000, 2013.

[7] J. Fridrich, “Symmetric ciphers based on two dimensional chaotic maps,” International Journal of Bifurcation & Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.

[8] T. G. Gao and Z. Q. Chen, “A new image encryption algorithm based on hyper-chaos,” Physics Letters A, vol. 372, no. 4, pp. 394–400, 2008.

[9] L. M. Jawad and G. Sulong, “Chaotic mapembedded blowfish algorithm for security enhancement of colour image encryption,” Nonlinear Dynamics, vol. 81, no. 4, pp. 1–15, 2015.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details